СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

***Харченко О.К.**, магистр, Харьковский национальный университет городского хозяйства имени О.Н. Бекетова*

Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов заказчика от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения служебной информации, обеспечение нормальной производственной деятельности всех подразделений объекта. Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Трудно представить, что с таким количеством и разнообразием технических и программных средств, могут возникнуть проблемы с созданием эффективной системы информационной безопасности компании. Но проблемы, все-таки существуют и относятся, скорее всего, к организационно-финансовым.

Первой и самой большой проблемой создания системы информационной безопасности является отсутствия понимания у руководства компании необходимости создания такой системы. Многие руководители компаний не осознают, что создавать систему информационной безопасности просто необходимо, но период уделения недостаточного внимания этому вопросу длится, как правило, не долго - до первого серьезного инцидента.

Вторая проблема создания системы информационной безопасности – отсутствие достаточного количества финансовых средств. Невыделение минимального бюджета для создания системы информационной безопасности встречается также очень часто. Лучше уж вообще не начинать создания системы информационной безопасности и знать о возможных угрозах, чем что-то предпринять и наслаждаться иллюзией защищенности. К примеру, в США и странах Евросоюза на создание системы информационной безопасности и поддержание ее в актуальном состоянии выделяется от 30% прибыли компании. У нас же если финансы и выделяются, то разово и в недостаточном количестве. Таких средств может хватить разве, что на продление лицензии на антивирус. И лишь некоторые компании, которых можно считать скорее исключением из правил, планируют и принимают бюджет своей системы информационной безопасности исходя из реальных потребностей.

И, наверное, самой опасной проблемой создания системы информационной безопасности является ситуация, когда есть понимания проблемы руководством компании, в наличии необходимые средства, но создание системы информационной безопасности поручают специалистам, не имеющим ни соответственного образования, ни достаточного опыта.

Зачастую создание системы информационной безопасности возлагают на системных администраторов или на отдел технической поддержки. Те, в свою очередь, создание системы информационной безопасности расценивают как установку и настройку файрвола и антивируса. И рапортуют перед руководством о том, что система информационной безопасности создана! А ведь тандем файрвол - антивирус далеко не является панацеей от проникновения из вне. Наличие внутреннего злоумышленника, зачастую, вообще не берется во внимание. А ведь к статистике, которая говорит о том, что 80% нарушений совершаются внутренними злоумышленниками, следует прислушиваться. Еще чаще без должного внимания остаются каналы связи. И переписка руководства компании с партнерами, менеджеров проектов с основными клиентами остается не защищенной.

Информационная безопасность информационных систем – состояние информационных систем, при котором обрабатываемая информация сохраняет конфиденциальность, доступность, целостность, соблюдаются правила и порядок разграничения доступа к информации и оборудованию, замены и ремонта оборудования, резервирования и восстановления информации, доступа в помещение и т.д.

Информационная безопасность информационных систем не зависит от класса ИС (одномашинный комплекс, локальная сеть, распределенные сети).

Информационная безопасность информационных систем зависит от физической, технической, программной среды, среды пользователей и четкой регламентации всех процессов жизнедеятельности компании

Угрозы информационной безопасности – любые обстоятельства или действия, которые могут быть причиной нарушения безопасности информации или нанести ущерб информационной системе.

Информационная безопасность предприятия – такая же важная составляющая бизнес-процессов, как и производственное оборудование, квалифицированный персонал, документооборот и т.д. Информационная безопасность предприятия направлена на предотвращение или минимизацию нанесения ущерба от реализации определенных угроз конфиденциальной информации предприятия. Информационная безопасность предприятия во многом зависит от степени понимания ее важности и необходимости руководством. Очень часто руководство предприятий под информационной безопасностью понимают лишь охрану периметра и организацию контрольно-пропускного пункта. Этот подход может быть оправдан, если затраты на организацию информационной безопасности не сопоставимы с убытками предприятия от реализации угроз ИБ. Ведь давно не секрет, что для создания эффективной системы информационной безопасности на предприятии необходимы капиталовложения и порой не маленькие, польза от которых на первый взгляд не видна. На предприятиях, где основные бизнес-процессы реализуются в автоматизированных информационных системах, отсутствие мер и средств информационной безопасности может привести как к огромным убыткам, так и к полной остановке.

Создание системы информационной безопасности заключается в разработке и внедрении мероприятий, правил, требований, ограничений, инструкций, нормативных документов, технических и программных средств для обеспечения определенного уровня информационной безопасности компании.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.